

Содержание

Глава 1. Хакинг. Понимание причин взлома.....13

- 1.1. КТО ЕСТЬ ХАКЕР..... 14
- 1.2. ЗАЧЕМ ВЗЛАМЫВАЮТ САЙТЫ..... 15
- 1.3. ПОЧЕМУ ВЗЛАМЫВАЮТСЯ САЙТЫ..... 16

Глава 2. Настройка веб-сервера.....19

- 2.1. УСТАНОВКА И НАСТРОЙКА APACHE..... 20
- 2.2. УСТАНОВКА СЕРВЕРА БАЗ ДАННЫХ. СОЗДАНИЕ БАЗЫ ДАННЫХ И ПОЛЬЗОВАТЕЛЯ..... 23
- 2.3. УСТАНОВКА И НАСТРОЙКА PHP. ВЫБОР ВЕРСИИ..... 25
- 2.4. ДИРЕКТИВЫ ФАЙЛА КОНФИГУРАЦИИ APACHE..... 29
- 2.5. НАСТРОЙКА ВИРТУАЛЬНЫХ УЗЛОВ ВЕБ-СЕРВЕРА..... 41
- 2.6. ДИРЕКТИВА USERDIR И КАТАЛОГИ ПОЛЬЗОВАТЕЛЕЙ..... 43
- 2.7. УСКОРЯЕМ ВЕБ-СЕРВЕРЫ. ТОНКАЯ НАСТРОЙКА APACHE..... 44
- 2.8. ЗАЩИТА СЕРВЕРА APACHE..... 45

Глава 3. Хакинг. Essentials.....47

- 3.1. САЙТ ИЛИ ВЕБ-ПРИЛОЖЕНИЕ..... 48

3.2. ЦЕЛИ АТАКИ.....	49
3.3. ЧТО ЕСТЬ УЯЗВИМОСТЬ	50
Пример 1: шаблон "двоеточие"	51
Пример 2: обход пути	51
Пример 3: cgi-bin.....	51
Пример 4: удаленное выполнение.....	52
3.4. НЕОБХОДИМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ	52
3.5. ЭТАПЫ АТАКИ	53
3.6. РЕАЛЬНЫЙ ПРИМЕР АТАКИ.....	53
3.6.1. Выбираем оптимальный способ.....	54
Способ 1. Друзья друзей	54
Способ 2. Сервисы накрутки	54
Способ 3. Накрутка с помощью анонимайзеров.....	54
Способ 4. Взлом сценария для голосования	54
3.6.2. Относительно легальные способы накрутки	55
Накрутка с помощью анонимайзеров	55
Анонимные прокси.....	56
3.6.3. Ломаем голосовалку	59
3.6.4. Автоматизируем.....	62

Глава 4. Сбор информации.....	65
--------------------------------------	-----------

4.1. ОБЩЕДОСТУПНЫЕ САЙТЫ.....	67
4.2. ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ДОМЕНЕ	67
4.3. КОМАНДА <i>HOST</i>	69
4.4. КОМАНДА <i>DIG</i>	70
4.5. ОЧЕНЬ ПОЛЕЗНЫЙ ИНСТРУМЕНТ — <i>DEEPMAGIC INFORMATION GATHERING TOOL (DMITRY)</i>	71

4.6. КОМАНДА <i>TRACEROUTE</i>	75
4.7. ИНСТРУМЕНТ <i>METAGOOFIL</i>	77
4.8. ПОЛУЧЕНИЕ ИНФОРМАЦИИ ИЗ ФАЙЛА <i>ROBOTS.TXT</i>	78
4.9. СКАНЕР <i>NMAP</i>	79
4.10. СКАНЕР <i>NIKTO</i>	81

Глава 5. Burp Suite для разведки и сканирования веб-приложения.....	85
--	-----------

5.1. ВВЕДЕНИЕ В <i>BURP SUITE</i>	86
5.2. ЗАПУСК И СОЗДАНИЕ ПРОЕКТА.....	88
5.3. НАСТРОЙКА ПРОКСИ	90
5.4. ВКЛАДКА <i>TARGET</i>	92
5.5. ИНСТРУМЕНТ <i>INTRUDER</i>	92

Глава 6. SQL-инъекции.....	103
-----------------------------------	------------

6.1. ВВЕДЕНИЕ В SQL-ИНЪЕКЦИИ	104
6.2. ПРИМЕР SQL-ИНЪЕКЦИИ.....	108
6.3. ПОИСК ЖЕРТВЫ	111
6.4. ИНСТРУМЕНТ <i>SQLMAP</i>	113

Глава 7. Атака обхода пути.....	119
--	------------

7.1. ПРИНЦИП АТАКИ.....	120
7.2. АТАКА НА PHP-ПРИЛОЖЕНИЕ.....	121

7.3. ОБХОД КАТАЛОГА С КОДИРОВКОЙ URI..... 122

7.4. ЗАЩИТА ОТ ОБХОДА КАТАЛОГА..... 123

Глава 8. Взлом пользователя веб-сервера.....125

8.1. КТО И ЗАЧЕМ ВЗЛАМЫВАЕТ АККАУНТЫ..... 126

8.2. СБОР ИНФОРМАЦИИ 129

8.3. МЕТОДЫ ВЗЛОМА..... 133

 8.3.1. Взлом электронной почты..... 133

 8.3.2. Социальный инжиниринг 133

 8.3.3. Перебор пароля 134

 8.3.4. Фишинг, или фейковая страничка. Очень подробное руководство 137

 8.3.5. Клавиатурный шпион 151

 8.3.6. Подмена DNS 152

Глава 9. Атаки на отказ (D/DoS).....155

9.1. АТАКА НА ОТКАЗ..... 156

9.2. ПРИЧИНЫ ПРОВЕДЕНИЯ АТАК НА ОТКАЗ..... 159

9.3. КЛАССИФИКАЦИЯ DOS-АТАК 160

9.4. УТИЛИТЫ ДЛЯ ОРГАНИЗАЦИИ АТАКИ НЕ ОТКАЗ..... 161

Глава 10. Атака DNS Hijacking.....163

10.1. ЧТО ТАКОЕ DNS HIJACKING 164

10.2. ТИПЫ АТАКИ..... 165

10.3. ПЕРЕНАПРАВЛЕНИЕ, ИЛИ DNS-СПУФИНГ 166

10.4. ПЕРЕХВАТ DNS И ВЗЛОМ ВЕБ-САЙТА.....	166
---	-----

Глава 11. Защита виртуального сервера.....	169
---	------------

11.1. МЕНЯЕМ ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ <i>ROOT</i>	170
--	-----

11.2. СОЗДАЕМ ОБЫЧНОГО ПОЛЬЗОВАТЕЛЯ.....	171
--	-----

11.3. УСТАНОВКА УДОБНОГО РЕДАКТОРА	172
--	-----

11.4. ПРЕВРАЩАЕМ ОБЫЧНОГО ПОЛЬЗОВАТЕЛЯ В АДМИНИСТРАТОРА... ..	173
---	-----

11.5. ЗАПРЕЩАЕМ ВХОД КАК <i>ROOT</i> ПО <i>SSH</i>	174
--	-----

11.6. МЕНЯЕМ ПОРТ <i>SSH</i>	175
------------------------------------	-----

11.7. <i>SSH</i> -ВХОД ПО КЛЮЧУ.....	175
--------------------------------------	-----

11.8. НАСТРОЙКА БРАНДМАУЭРА	177
-----------------------------------	-----

11.8.1. Базовая настройка	177
---------------------------------	-----

11.8.2. Создание правил для сервисов	179
--	-----

11.8.3. Разрешаем IP-адреса.....	180
----------------------------------	-----

11.8.4. Запрещаем IP-адреса и службы	181
--	-----

11.8.5. Удаление и сброс правил.....	181
--------------------------------------	-----

11.9. ПОМНИМ О РЕЗЕРВНЫХ КОПИЯХ.....	182
--------------------------------------	-----

Глава 12. Фишинг.....	187
------------------------------	------------

12.1. ЧТО ТАКОЕ ФИШИНГ	188
------------------------------	-----

12.2. РЕАЛЬНЫЙ ПРИМЕР	191
-----------------------------	-----

Глава 13. Брутфорсинг.....	197
-----------------------------------	------------

13.1. ГРУБАЯ СИЛА	198
-------------------------	-----

13.2. ПОДБОР ПАРОЛЯ ПО ХЕШУ 199

13.3. БРУТФОРСИНГ MYSQL..... 202

13.4. БРУТФОРСИНГ SSH..... 204

Глава 14. Инструменты для поиска уязвимостей веб-сервера.....207

14.1. СКАНЕРЫ УЯЗВИМОСТЕЙ..... 208

14.2. СКАНЕР SNIPER..... 209

14.3. СКАНЕР NESSUS..... 210

14.4. OWASP ZAP..... 211

14.5. СКАНЕР VEGA..... 212

14.6. СКАНЕР KUBE-HUNTER..... 213

14.7. SKIPFISH..... 215

Глава 15. Использование Metasploit для взлома.....221

15.1. ЗНАКОМСТВО С METASPLOIT 222

15.2. СТРУКТУРА ФРЕЙМВОРКА 224

15.3. БАЗОВАЯ ТЕРМИНОЛОГИЯ..... 225

15.4. КОНФИГУРАЦИИ ФРЕЙМВОРКА И ОСНОВНЫЕ КОМАНДЫ 227

15.5. КОНФИГУРАЦИЯ МОДУЛЕЙ 228

15.6. ПЕРВЫЙ ЗАПУСК METASPLOIT 229

15.7. ПРАКТИЧЕСКОЕ ИСПОЛЬЗОВАНИЕ КОМАНД METASPLOIT 234

15.7.1. Команда *help* — получение справки..... 234

15.7.2. Команда <i>use</i> — выбор модуля для использования	235
15.7.3. Команда <i>show</i> — показ сущностей	236
15.7.4. Команды <i>set</i> и <i>setg</i> — установка значений переменных	241
15.7.5. Команда <i>check</i> — проверка целевой системы.....	242
15.7.6. Команда <i>back</i> — возврат	243
15.7.7. Команда <i>run</i> — запуск эксплоита	243
15.7.8. Команда <i>resource</i> — определение ресурса.....	244
15.7.9. Команда <i>irb</i>	244

15.8. ПРАКТИЧЕСКИЙ ПРИМЕР 1: ВЗЛАМЫВАЕМ СТАРЕНЬКИЙ СЕРВЕР WINDOWS 2008 С ПОМОЩЬЮ ЭКСПЛОИТА АНБ	245
15.9. ПРАКТИЧЕСКИЙ ПРИМЕР 2: ХАКАЕМ СОВРЕМЕННЫЕ СИСТЕМЫ — WINDOWS SERVER 2016 И WINDOWS 10	249

Глава 16. Взлом WordPress: отдельный разговор.....255

16.1. ПОЧЕМУ ИМЕННО WORDPRESS	256
16.2. ПРИЗНАКИ ВЗЛОМА: КАК ПОНЯТЬ, ЧТО ВАШ WORDPRESS ВЗЛОМАН	260
16.2.1. Неуспешный вход	260
16.2.2. Вредоносный контент.....	260
16.2.3. Подозрительная активность.....	261
16.2.4. Существенная просадка в трафике	261
16.2.5. Странные результаты поисковой машины.....	261
16.2.6. Перестали отправляться e-mail с сайта	262
16.2.7. Сайт не открывается, или начальная страница отличается от привычной	262
16.2.8. Подозрительные файлы.....	262
16.2.9. Новые пользователи	262
16.2.10. Новые задачи в планировщике	263
16.3. ОСНОВНЫЕ ПРИЧИНЫ ВЗЛОМА WORDPRESS-САЙТОВ	263
16.3.1. Небезопасный веб-хостинг	263
16.3.2. Слабые пароли	263

16.3.3. Незащищенный доступ к панели управления сайтом.....	264
16.3.4. Ненадлежащим образом установленные права доступа к файлам и папкам.....	265
16.3.5. Использование устаревшей версии WordPress.....	266
16.3.6. Устаревшие версии плагинов и тем оформления.....	267
16.3.7. Использование FTP вместо SFTP/SSH.....	267
16.3.8. Учетная запись <i>admin</i>	267
16.3.9. "Нулевые" темы и плагины.....	268
16.3.10. Утечка файла wp-config.php.....	268
16.4. КАК МОЖНО ВЗЛОМАТЬ WORDPRESS-САЙТ.....	268
16.4.1. Создание новых пользователей через FTP.....	268
16.4.2. Файл functions.php.....	269
16.4.3. Использование панели управления хостингом.....	270
16.4.4. Метод грубой силы.....	270
16.4.5. XSS-атака.....	273
16.4.6. SQL-инъекция.....	274
16.4.7. Черный вход.....	276
16.5. ИНСТРУМЕНТ WPSCAN.....	277

<p>Глава 17. Что такое Kali Linux и как его использовать для взлома.....279</p>
--

17.1. ВКРАТЦЕ О KALI.....	280
17.2. ГДЕ СКАЧАТЬ И КАК УСТАНОВИТЬ KALI LINUX.....	281
17.3. ОБСЛУЖИВАНИЕ СИСТЕМЫ.....	294
17.3.1. Обслуживание источников пакетов.....	294
17.3.2. Ошибка " <i>The disk contains an unclean file system (0, 0). Metadata kept in Windows cache, refused to mount</i> ".....	295
17.3.3. Регулярная очистка системы.....	295